

# A New Approach to the Main Problem of Subspace Coding

Liu Haiteng

Department of Information Science  
and Electronics Engineering  
Zhejiang University, 38 Zheda Road  
310027 Hangzhou, China  
Email: liuhaiteng@zju.edu.cn

Thomas Honold

Department of Information Science  
and Electronics Engineering  
Zhejiang University, 38 Zheda Road  
310027 Hangzhou, China  
Email: honold@zju.edu.cn

**Abstract**—Subspace codes form the appropriate mathematical setting for investigating the Koetter-Kschischang model of fault-tolerant network coding. The Main Problem of Subspace Coding asks for the determination of a subspace code of maximum size (proportional to the transmission rate) if the remaining parameters are kept fixed. We describe a new approach to finding good subspace codes, which surpasses the known size limit of lifted MRD codes and is capable of yielding an alternative construction of the currently best known binary subspace code of packet length 7, constant dimension 3 and minimum subspace distance 4.

**Index Terms**—Subspace code, Main Problem of Subspace Coding, network coding, linear operator channel, MRD code, parallelism

## I. INTRODUCTION

Let  $q > 1$  be a prime power. A  $q$ -ary (constant-dimension) subspace code with parameters  $(v, M, d; k)$  is a set  $\mathcal{C} = \{U_1, \dots, U_M\}$  of  $M$  distinct  $k$ -dimensional subspaces  $U_i$  of the “ambient” vector space  $\mathbb{F}_q^v$  (over  $\mathbb{F}_q$ ) with minimum subspace distance  $d_s(\mathcal{C}) = \min\{d_s(U_i, U_j); 1 \leq i < j \leq M\} = d$ . Here the *subspace distance* of  $U$  and  $V$  is defined in general as  $d_s(U, V) = \dim(U + V) - \dim(U \cap V)$  and in the special case  $\dim(U) = \dim(V) = k$  reduces to  $d_s(U, V) = 2k - 2\dim(U \cap V)$ . In particular,  $d = 2\delta$  is always even and  $t = k - \delta + 1$  is the smallest integer such that every  $t$ -dimensional subspace of  $\mathbb{F}_q^v$  is contained in at most one member of  $\mathcal{C}$ .

The *Main Problem of (constant-dimension) Subspace Coding* can be described as follows:

Given a prime power  $q > 1$  and positive integers  $v, k, \delta$  with  $2 \leq \delta \leq k \leq v/2$ , determine the largest cardinality  $M$  of a  $q$ -ary  $(v, M, 2\delta; k)$  subspace code. This cardinality will be denoted by  $A_q(v, 2\delta; k)$ .

Restriction to the case  $k \leq v/2$  entails no loss, since the map  $U \mapsto U^\perp$  (orthogonality being taken with respect to the usual dot product) preserves the subspace distance and hence identifies  $q$ -ary  $(v, M, 2\delta; k)$  subspace codes with  $(v, M, 2\delta; v - k)$  subspace codes.

The Main Problem of Subspace Coding arose in connection with the Koetter-Kschischang model of fault-tolerant network coding [1] (see [2] for an introduction), which uses appropriate subspace codes to encode messages before transmission over an ordinary network-coded (implemented by some form of random linear network coding) packet network. Subspace codes with large size and large minimum distance account for large transmission rate and good error-correcting capabilities, respectively, and the determination of the best such codes is thus of particular importance.

The Main Problem of Subspace Coding is akin to its classical counterpart, the Main Problem of Algebraic Coding Theory, which asks for the determination of the best linear codes over  $\mathbb{F}_q$  relative to the Hamming distance and forms the mathematical abstraction of the engineering problem of finding the best point-to-point channel codes. The Main Problem of Subspace Coding is much more difficult, however, since the set of all subspaces of  $\mathbb{F}_q^v$  does not admit a group structure compatible with the subspace metric. Hence there is no suitable notion of “linearity” for subspace codes, which could be exploited.

In Finite Geometry language, a  $q$ -ary  $(v, M, 2\delta; k)$  subspace code is a set  $\mathcal{C}$  of  $M$  distinct  $(k - 1)$ -flats in the projective geometry  $\text{PG}(v - 1, q)$  such that any  $(k - \delta)$ -flat is contained in at most one member of  $\mathcal{C}$  and some  $(k - \delta - 1)$ -flat is contained in at least two members of  $\mathcal{C}$ . The Main Problem of Subspace Coding is therefore equivalent to the packing problem for  $(k - 1)$ -flats in  $\text{PG}(v - 1, q)$  when these flats are identified with sets of  $(t - 1)$ -flats (all  $(t - 1)$ -flats contained in the given  $(k - 1)$ -flat), where  $t = k - \delta + 1$ . Thus it comes as no surprise that most of the known results on the Main Problem, at the time of its advent, had been obtained by Finite Geometers. With a few exceptions, these results pertain to the extremal case  $\delta = k$  of pairwise disjoint  $(k - 1)$ -flats, so-called spreads or partial spreads, and really satisfactory results were known only for the “line” case  $k = 2$ .

While some progress has been made since then, the Main Problem (unlike its classical counterpart) is still widely open. Koetter and Kschischang, in their seminal

paper [1], used so-called maximum-rank-distance (MRD) codes, found earlier by Delsarte [3], Gabidulin [4] and Roth [5], and a suitable lifting construction to produce a good approximation to optimal subspace codes for general parameter sets. Etzion and Silberstein [6] (cf. [7] for the latest improvements) introduced the echelon-Ferrers construction as a method to augment lifted MRD (LMRD) codes by further subspaces, while keeping their minimum distance. Further constructions of subspace codes for specific parameter sets, improving on the general methods mentioned so far but usually relying heavily on computer searches, can be found in [8], [9], [10]. The numbers  $A_q(v, 2\delta; k)$  have been determined exactly for  $v \leq 5$  (all  $q$ ) and in the binary case also for  $v = 6$ . This includes  $A_q(4, 4; 2) = q^2 + 1$  (realized by a line spread in  $\text{PG}(3, q)$ ),  $A_q(5, 4; 2) = q^3 + 1$  (the maximal size of a partial line spread in  $\text{PG}(4, q)$ ; cf. [11]), and  $A_2(6, 4; 3) = 77$  (realized by 5 different isomorphism types of optimal subspace codes; cf. [12]). Moreover, from the recent ground-breaking discovery of the first 2-analogue of a Steiner triple system in [13] it is also known that  $A_2(13, 4; 3) = 1597245$ .

Our contribution in this paper is a new approach to the construction of good subspace codes, which has its origin in the observation made in [12] that removing certain subcodes from an LMRD code may result in the opportunity to add even more subspaces to the expurgated LMRD code, thereby surpassing the size of the LMRD code, as well as any other subspace code containing an LMRD code.

In contrast with the construction of a binary  $(6, 77, 4; 3)$  subspace code of Type A in [12], which used the smallest possible set of removed codewords, we propose to remove a much larger set of codewords from an LMRD code. As it turns out, our approach is capable of constructing a binary  $(7, 329, 4; 3)$  subspace code, equalizing the current record size and providing an alternative construction of a code with  $M = 329$  for the parameter set  $q = 2$ ,  $v = 7$ ,  $k = 3$ ,  $d = 4$ ; cf. [10].

The main result is described in Section V. Section II contains information about a putative binary  $(7, 381, 4; 3)$  subspace code, whose existence/non-existence is a famous unsolved problem, and the subsequent two sections contain preparatory material for our main result and related subspace code constructions.

Throughout the paper we will use basic concepts and terminology from Finite Geometry. Readers are referred to [14], [15], [16] for the relevant background information and any unexplained terms.

## II. THE PUTATIVE 2-ANALOGUE OF THE FANO PLANE

An easy double-counting argument yields the bound  $M \leq 381$  for any binary  $(7, M, 4; 3)$  subspace code  $\mathcal{C}$ . If equality holds then with  $t = 2$ ,  $k = 3$ ,  $v = 7$  every  $t$ -dimensional subspace of  $\mathbb{F}_2^v$  must be contained in precisely one  $k$ -dimensional subspace (codeword) of  $\mathcal{C}$ . Such a structure is known as a Steiner system over  $\mathbb{F}_2$ , and in

the particular case  $(t, k, v) = (2, 3, 7)$  under consideration has been named “2-analogue of the Fano plane  $\text{PG}(2, 2)$ ”, since  $\text{PG}(2, 2)$  is the unique ordinary Steiner system with these parameters. Steiner systems over finite fields (and, more generally, combinatorial designs over finite fields) were introduced by Thomas [17], who then was able to show that a putative 2-analogue of the Fano plane cannot be constructed using the obvious idea of combining three plane orbits (of size 127) of a Singer group of  $\text{PG}(6, 2)$ .

In an attempt to construct such a 2-analogue  $\mathcal{C}$ , one can proceed as follows. Out of the  $\begin{bmatrix} 7 \\ 4 \end{bmatrix}_2 = 11811$  solids in  $\text{PG}(6, 2)$  (4-dimensional subspaces of  $\mathbb{F}_2^7$ ),  $15 \times 381 = 5715$  should contain a codeword of  $\mathcal{C}$  and 6096 should not contain a codeword of  $\mathcal{C}$ . We now fix one such solid as the subspace  $S = (0, 0, 0, *, *, *, *)$  of  $\mathbb{F}_2^7$  and count the number of codewords of  $\mathcal{C}$  meeting  $S$  in a subspace of fixed dimension.

*Lemma 1:* Suppose  $\mathcal{C}$  is a putative 2-analogue of the Fano plane and  $a_i = \#\{U \in \mathcal{C}; \dim(U \cap S) = i\}$  for  $0 \leq i \leq 3$  is the so-called *intersection vector of  $S$  with respect to  $\mathcal{C}$* . Then  $(a_1, a_1, a_2, a_3)$  is either  $(128, 224, 28, 1)$  or  $(136, 210, 35, 0)$ , depending on whether  $S$  contains a codeword of  $\mathcal{C}$  or not, respectively.

This lemma also follows from the general theory of intersection numbers for subspace designs, as developed in [18].

*Proof:* We prove only the case where  $S$  does not contain a codeword of  $\mathcal{C}$ , i.e.  $a_3 = 0$ . The other case is proved similarly.

Each of the  $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_2 = 35$  lines in  $S$  is contained in exactly one codeword and the 35 codewords obtained in this way are distinct, since the planes in  $S$  spanned by two of the lines are not in  $\mathcal{C}$ . This gives  $a_2 = 35$ . Double-counting yields that each point of  $\text{PG}(6, 2)$  is contained in 21 codewords. Hence each of the 15 points in  $S$  must be contained in 7 codewords meeting  $S$  in a line and in 14 codewords meeting  $S$  in a point. Consequently,  $a_1 = 15 \cdot 14 = 210$  and  $a_0 = 381 - 35 - 210 = 136$ . ■

Further information about a putative 2-analogue  $\mathcal{C}$  of the Fano plane can be derived along these lines. For example, every hyperplane (5-flat) of  $\text{PG}(6, 2)$  must contain exactly 45 codewords, every 4-flat exactly 5 codewords, and every point-hyperplane flag  $(p, H)$  must be incident with exactly 5 codewords  $U$  (i.e.,  $p \subset U \subset H$ ). All this is not yet sufficient, however, to narrow down the number of possible configurations, so that a computer search becomes feasible.

## III. AUGMENTED LMRD CODES

Suppose  $k, m, n$  are positive integers with  $k \leq m \leq n$ .<sup>1</sup> An  $(m, n, k)$  *maximum rank distance (MRD)* code over  $\mathbb{F}_q$  is a set  $\mathcal{A} = \{\mathbf{A}_1, \dots, \mathbf{A}_{q^{nk}}\}$  of  $q^{nk}$  distinct matrices in  $\mathbb{F}_q^{m \times n}$  having minimum rank distance  $d_r(\mathcal{A}) = \min\{\text{rk}(\mathbf{A}_i - \mathbf{A}_j); 1 \leq i < j \leq q^{nk}\} = n - k + 1$ . An argument similar to that used in the proof of the

<sup>1</sup>The symbol ‘ $k$ ’ has a different meaning within this section.

Singleton bound for ordinary block codes shows that  $q$ -ary  $(m, n, k = n - d + 1)$  MRD codes in  $\mathbb{F}_q^{m \times n}$  have maximum size subject to the requirement  $d_r(\mathcal{A}) \geq d$ , accounting for their name. According to [3], [4], [5], MRD codes exist for all admissible parameters  $q, k, m, n$  and may be constructed using a  $q$ -analogue of the familiar Reed-Solomon code construction (employing linearized polynomials in place of ordinary polynomials).

As shown in [1], [19], the map  $\lambda$  sending a matrix  $\mathbf{A} \in \mathbb{F}_q^{m \times n}$  to the row space of  $(\mathbf{I}_m | \mathbf{A}) \in \mathbb{F}_q^{m \times (m+n)}$  satisfies  $d_s(\lambda(\mathbf{A}), \lambda(\mathbf{B})) = 2d_r(\mathbf{A}, \mathbf{B})$  (i.e. constitutes a “scaled isometry” with scale factor 2). This immediately gives that for any  $q$ -ary  $(m, n, k)$  MRD code  $\mathcal{A}$  the image  $\lambda(\mathcal{A})$  forms a  $q$ -ary  $(m+n, q^{nk}, 2(n-k+1); m)$  subspace code, a so-called *lifted maximum rank distance (LMRD) code*.

We are interested in the case  $q = 2$ ,  $(m, n, k) = (3, 4, 2)$ , since an MRD code with these parameters gives rise to a binary  $(7, 256, 4; 3)$  subspace code, providing a good approximation to binary optimal  $(7, M, 4; 3)$  subspace codes. The standard MRD code with these parameters is the “Gabidulin code”

$\mathcal{G} = \{a_0x + a_1x^2; a_0, a_1 \in \mathbb{F}_{16}\}$ , viewed as a set of  $\mathbb{F}_2$ -linear transformations  $W \rightarrow \mathbb{F}_{16}$ ,  $x \mapsto a_0x + a_1x^2$  on a fixed 3-dimensional  $\mathbb{F}_2$ -subspace  $W$  of  $\mathbb{F}_{16}$ , which is conveniently taken as the set of all elements  $u \in \mathbb{F}_{16}$  of absolute trace zero (i.e.  $\text{Tr}(u) = \text{Tr}_{\mathbb{F}_{16}/\mathbb{F}_2} = u + u^2 + u^4 + u^8 = 0$ ). If  $\mathbb{F}_{16}$  is constructed as  $\mathbb{F}_2[\alpha]$  subject to  $\alpha^4 + \alpha + 1 = 0$ , we have  $W = \{0, 1, \alpha, \alpha^2, \alpha^4, \alpha^5, \alpha^8, \alpha^{10}\}$ . An explicit representation of  $\mathcal{G}$  by binary  $3 \times 4$  matrices can then be obtained through fixing bases of  $W$  and  $\mathbb{F}_{16}$  over  $\mathbb{F}_2$  and using coordinates with respect to these bases.

In our implementation we have used  $W = \langle 1, \alpha, \alpha^2 \rangle$ ,  $\mathbb{F}_{16} = \langle 1, \alpha, \alpha^2, \alpha^3 \rangle$ . Then the  $4 \times 4$  matrices corresponding to  $x \mapsto \alpha x$  and  $x \mapsto x^2$  (which determine all 256 matrices of the  $4 \times 4$  matrix representation of  $\mathcal{G}$ ) are

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

respectively, and the  $3 \times 4$  matrix representation of  $\mathcal{G}$  is obtained by deleting the last row of all 256 matrices. The rank of the 255 nonzero  $3 \times 4$  matrices (and hence the subspace distance between any two distinct  $3 \times 4$  matrices) is at least 2, since a nonzero  $\mathbb{F}_2$ -linear transformation  $W \rightarrow \mathbb{F}_{16}$ ,  $x \mapsto a_0x + a_1x^2$  has a kernel of dimension  $\leq 1$ . Applying  $\lambda$  to the 256 selected  $3 \times 4$  matrices produces the required  $(7, 256, 4; 3)$  LMRD code  $\lambda(\mathcal{G})$  as an explicit set of 256 generating matrices in  $\mathbb{F}_2^{3 \times 7}$ .

*Remark 1:* Sometimes it is more convenient to work with the polynomials in  $\mathcal{G}$  directly rather than with their representing matrices. A basis-independent representation of  $\lambda(\mathcal{G})$  can be obtained as follows: Take  $W \times \mathbb{F}_{16} \cong \mathbb{F}_2^7$  as the ambient vector space and the codewords of  $\lambda(\mathcal{G})$  as the *graphs* (in the sense of Real Analysis) of the linear maps

induced by the polynomials in  $\mathcal{G}$ . In this representation the 256 codewords of  $\lambda(\mathcal{G})$  are

$$G(a_0, a_1) = \{(x, a_0x + a_1x^2); x \in W\}, \quad a_0, a_1 \in \mathbb{F}_{16}.$$

Since  $x \mapsto a_0x + a_1x^2$  is  $\mathbb{F}_2$ -linear, it is clear that each set  $G(a_0, a_1)$  is a 3-dimensional  $\mathbb{F}_2$ -subspace of  $W \times \mathbb{F}_{16}$ . Moreover, using coordinates in  $W \times \mathbb{F}_{16}$  with respect to the ordered basis  $(1, 0), (\alpha, 0), (\alpha^2, 0), (0, 1), (0, \alpha), (0, \alpha^2), (0, \alpha^3)$  identifies the spaces  $G(a_0, a_1)$  with the codewords of  $\lambda(\mathcal{G})$  as introduced earlier.

It has been shown in [20] using the concept of “pending dots” that the lifted  $(7, 256, 4; 3)$  Gabidulin code  $\lambda(\mathcal{G})$  can be augmented by 35 further subspaces to a  $(7, 291, 4; 3)$  subspace code. Any further enlargement is impossible, since the codewords of  $\lambda(\mathcal{G})$  cover all  $7 \times 256 = 1792$  lines disjoint from the special solid  $S = (0, 0, 0, *, *, *, *)$ , so that additional codewords must meet  $S$  at least in a line, which clearly conflicts with some of the 35 codewords outside  $\lambda(\mathcal{G})$  already chosen.

We close this section by providing a different geometric construction of the augmented  $(7, 291, 4; 3)$  subspace code, which seems to be worth mentioning. It is known that  $\text{PG}(3, 2)$  admits a line packing (parallelism)  $\mathcal{S} = \{\mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{S}_4, \mathcal{S}_5, \mathcal{S}_6\}$ , i.e. the 35 lines are partitioned into 7 spreads  $\mathcal{S}_i$ , each spread containing 5 pairwise disjoint lines.<sup>2</sup> Now take seven points  $p_i$ ,  $0 \leq i \leq 6$ , in  $\text{PG}(6, 2)$  such that the seven 4-flats  $\langle p_i, S \rangle$  are distinct (and hence represent all the 4-flats above  $S$ ). Connect a line  $L$  in  $S$  to  $p_i$  if  $L \in \mathcal{S}_i$ , and augment  $\lambda(\mathcal{G})$  by the 35 planes  $\langle p_i, L \rangle$  obtained in this way. It is readily checked that the resulting subspace code  $\mathcal{C}$  of size 291 still has  $d_s(\mathcal{C}) = 4$ .

Using the known “cyclic” description of  $\mathcal{S}$  it is not hard to produce a list of the 35 additional codewords. In the basis-independent representation one can take  $p_0 = \mathbb{F}_2(1, 0) = \mathbb{F}_2 \times \{0\}$  and  $\mathcal{S}_0$  to consist of  $\{0\} \times \alpha^j \mathbb{F}_4$  for  $0 \leq j \leq 4$ , i.e. start with the 5 planes  $E(0, j) = \mathbb{F}_2 \times \alpha^j \mathbb{F}_4$ ,  $0 \leq j \leq 4$ , and generate the remaining codewords from these by applying the linear permutation  $\sigma = (0)(\alpha^{14})(1, \alpha, \alpha^2, \alpha^4, \alpha^5, \alpha^{10}, \alpha^8)(\alpha^7, \alpha^{13}, \alpha^9, \alpha^{12}, \alpha^{11}, \alpha^6, \alpha^3)$  of  $\mathbb{F}_{16}$  simultaneously to both coordinates of  $W \times \mathbb{F}_{16}$ . The resulting 35 additional codewords are

$$E(i, j) = \sigma^i(\mathbb{F}_2) \times \sigma^i(\alpha^j \mathbb{F}_4), \quad 0 \leq i \leq 6, 0 \leq j \leq 4.$$

The choice of a point of the special form  $p = \mathbb{F}_2(a, 0)$  in every additional plane is not mandatory, and in fact one could make 35 arbitrary choices for the second coordinates of these points.

#### IV. EXPURGATING THE LMRD CODE FIRST

From [12] we know that it makes sense to remove certain sets of codewords from the  $(7, 256, 4; 3)$  code  $\lambda(\mathcal{G})$ . The idea behind this approach is that the removal of  $M_0$  codewords from  $\lambda(\mathcal{G})$  “frees”  $7M_0$  lines disjoint from the special

<sup>2</sup>Such a line packing provides a solution to Kirkman’s School Girl Problem; see e.g. [21].

solid  $S$ , which are no longer covered by the expurgated subspace code, and hence can possibly be rearranged, four lines at a time, into “new planes”  $N$  of  $\text{PG}(6, 2)$  meeting  $S$  in a point. In the best case, it will be possible to add  $7M_0/4$  new planes to the expurgated subspace code, resulting in a subspace code of size  $256 - M_0 + 7M_0/4 = 256 + 3M_0/4$  that is superior to  $\lambda(\mathcal{G})$ .

The results in [12] imply that all  $7M_0$  free lines can be rearranged into new planes if the removed set of codewords has the form  $\lambda(\mathcal{R})$  for some (disjoint) union  $\mathcal{R} = \biguplus_{s=1}^t (f_s + \mathcal{T})$  of cosets of the following special 3-dimensional  $\mathbb{F}_2$ -subspace  $\mathcal{T}$  of  $\mathcal{G}$ :

$$\mathcal{T} = \{u^2x + ux^2; u \in W\}.$$

Any such choice of  $\mathcal{R}$  uniquely determines  $14t$  new planes meeting  $S$  in a point and covering, together with the codewords in the expurgated subspace code, each line disjoint from  $S$  exactly once. It remains to be checked whether the new planes  $N_i$  mutually satisfy the subspace distance condition  $d_s(N_i, N_j) \geq 4$  if  $i \neq j$ . Equivalently, if  $N_i$  and  $N_j$  pass through the same point  $s \in S$  then  $N_i \cap N_j = \{s\}$ . (For new planes passing through distinct points of  $S$  there is no further restriction.)

Using the computer algebra package SAGE ([www.sagemath.org](http://www.sagemath.org)), we have checked how many cosets of  $\mathcal{T}$  can be put into  $\mathcal{R}$  without violating the subspace distance condition for the resulting new planes. It turned out that the maximum is  $t = 2$  and  $\mathcal{R}$  can be taken as  $\{u^2x + ux^2; u \in \mathbb{F}_{16}\}$ . This results in a  $(7, 268, 4; 3)$  subspace code, which can be further augmented by 35 planes meeting  $S$  in a line (using the method described at the end of Section III with some specific choice of the points  $p_i$ ) to a  $(7, 303, 4; 3)$  subspace code.

A straightforward extension of the reasoning in [12] shows that the 28 new planes, obtained by rearranging the 112 lines in the planes  $G(u^2, u)$ ,  $u \in \mathbb{F}_{16}$ , corresponding to  $\mathcal{R}$ , meet  $S$  in the points  $\mathbb{F}_2(a^2b + ab^2)$  with  $a, b \in W$  nonzero and distinct, and have the basis-independent representation

$$N(Z, u) = \{(x, u^2x + ux^2 + y); x \in Z, y \in \mathbb{F}_2(a^2b + ab^2)\},$$

where  $Z = \langle a, b \rangle$  denotes one of the seven 2-dimensional  $\mathbb{F}_2$ -subspaces of  $W$  and  $u \in \mathbb{F}_{16}/Z$ .

From this we realized that the intersection points with  $S$  of the new planes determined by  $\mathcal{R}$  are simply the points on  $W$  (which forms a subplane of  $S$ ), and thus account for only 7 of the 15 points on  $S$ . This is in contrast with the construction in [12], which has  $\dim(S) = 3$  and new planes passing through every point of  $S$ .

Extending our scope to the “rotated” subspaces  $\mathcal{T}v = \{(u^2x + ux^2)v; u \in W, v \in \mathbb{F}_{16}^\times\}$ , we were able to overcome this restriction, but now had  $15 \times 32 = 480$  cosets to consider simultaneously. Moreover, cosets  $f + \mathcal{T}v$  for distinct  $v$  need no longer be disjoint, imposing an additional restriction.

The new problem can be viewed as a maximum clique problem in graph theory.<sup>3</sup> View every coset  $f + \mathcal{T}v$  as a vertex of an undirected graph  $G$ . If two cosets are disjoint and their subspace lifts have subspace distance at least 4 from each other, draw an edge between these two vertices. The clique number of  $G$  then gives the number of cosets  $f + \mathcal{T}v$  we can put into  $\mathcal{R}$ .

The clique number of  $G$  turned out to be 4 (again with the help of SAGE), i.e.  $4 \times 8 = 32$  planes can be removed in exchange for 56 new planes, resulting in a  $(7, 280, 4; 3)$  subspace code. The augmentation problem for this code can be modelled as a maximum clique problem as well, and we found this time that 34 further planes can be added to produce a  $(7, 314, 4; 3)$  subspace code.

## V. THE NEW APPROACH

From Section II we know that in order to qualify for a putative 2-analogue of the Fano plane, the “removed set” of subspaces of  $\lambda(\mathcal{G})$  should be much larger than those considered in the previous section—about half the size of  $\mathcal{G}$ . In the case where  $S$  does not contain a codeword (which can always be assumed by suitably changing the coordinate system), we should remove  $120 = 15 \cdot 8$  planes (i.e. 15 cosets  $f + \mathcal{T}v$ ) from  $\lambda(\mathcal{G})$  and replace these by  $210 = 14 \times 15$  new planes (14 new planes through each point of  $S$ ). A moment’s reflection shows that there is an obvious candidate for the corresponding removed set of matrices  $\mathcal{R}$ , viz. take

$$\mathcal{R} = \biguplus_{v \in \mathbb{F}_{16}^\times} (u^2x + ux^2 + \mathcal{T})v, \quad \text{where } \text{Tr}(u) = 1.$$

These 15 cosets are disjoint, since  $\mathcal{G}$  admits a partition into  $\{0\}$ ,  $\mathbb{F}_{16}^\times x$ ,  $\mathbb{F}_{16}^\times x^2$  and the 15 sets  $\{(u^2x + ux^2)v; u \in \mathbb{F}_{16}^\times\}$  with  $v \in \mathbb{F}_{16}^\times$ .

Using this set  $\mathcal{R}$  as the removed set, it is at least conceivable that the resulting  $7 \times 120 = 4 \times 210$  free lines can be rearranged into 210 new planes satisfying the subspace distance condition. This condition is in fact quite easy to check, since problems can occur only for the 14 new planes passing through a fixed point of  $S$ , and the 15 sets of 14 new planes determined in this way are isomorphic as subspace codes (since multiplication by  $v \in \mathbb{F}_{16}^\times$ , viewed as a Singer group acting on  $S = (0, 0, 0 | *, *, *, *)$ , identifies these sets).

The key question therefore is: What is the size of the largest clique in one of these 14-sets of new planes (say, the 14 new planes through  $p = \mathbb{F}_2(0, 0, 0 | 1, 0, 0, 0)$ )?

Using again a maximum clique model, we found that the clique number is  $11 < 14$  (hence a putative 2-analogue of the Fano plane cannot be constructed in this way), and the number of maximum cliques is 4. This yields a new subspace code of size  $M = 256 - 120 + 11 \times 15 = 301$ ,

<sup>3</sup>A *clique* in an undirected graph  $G = (V, E)$  is a subset  $C \subseteq V$  of the vertex set such that any two vertices in  $C$  are connected by an edge in  $E$ . A *maximum clique* is a clique of the largest possible size  $\#C$ , called the *clique number* of  $G$ .

subject to further augmentation by planes meeting  $S$  in a line or being contained in  $S$ . However, since there are 4 choices for the 11 new planes through each point of  $S$ , the total number of new  $(7, 301, 4; 3)$  subspace codes obtained in this way is  $4^{15} = 1073741824$ . It is impossible to check all these subspace codes for further augmentation in a reasonable amount of time. Instead we used a randomized search method (checking several thousands of cases) and found a maximum of 28 planes that can be added to some (in fact, many different) of the  $4^{15}$  subspace codes, resulting in a binary  $(7, 329, 4; 3)$  subspace code. This is our main result and equalizes the record set in [10].

## VI. CONCLUSION

We have outlined a new framework for the construction of good binary  $(v, M, 4; 3)$  subspace codes, which starts with a distinguished  $(v - 3)$ -dimensional subspace  $S$  of the ambient space  $\mathbb{F}_2^v$  and selects codewords based on their intersection dimension with  $S$ . The subspace codes constructed do not contain lifted MRD codes and hence are able to overcome the size limit imposed on such codes. We have worked out the case  $v = 7$  in detail and found that our framework is capable of yielding the largest known subspace codes in this case.

Several challenging questions arise from our work. Is it possible to construct the recently found 2-analogue of a Steiner triple system, a binary  $(13, 1597245, 4; 3)$  subspace code along these lines? For this the distinguished subspace  $S$  would be 10-dimensional and, as one can show, admit many different feasible intersection vectors  $(a_0, a_1, a_2, a_3)$ . There is, however, a particular choice for  $a_0$ , which is motivated by the example  $v = 7$  and determines the intersection vector completely:  $a_0 = 2^{19} + 2^9 = 524800 = 2^9 \times 5^2 \times 41$ ,  $a_1 = 916608 = 2^7 \times 3 \times 7 \times 11 \times 31$ ,  $a_2 = 152768 = 2^6 \times 7 \times 11 \times 31$ ,  $a_3 = 3069 = 3 \times 11 \times 31$ . Thus  $S$  would have to contain  $3069 = 3 \times 1023$  (three times the number of points in  $S$ ) codewords, and through each point  $p \in S$  there would be  $2^7 \times 7 = 896$  new planes meeting  $S$  in  $p$ . Is such a construction of a binary  $(13, 1597245, 4; 3)$  subspace code actually possible?

Further questions are those for the largest  $q$ -ary  $(7, M; 4; 3)$  subspace codes constructible by our method for prime powers  $q > 2$ , and for general lower bounds on the clique numbers of the graphs involved that could be used to derive an infinite family of, say, binary  $(v, M, 4; 3)$  subspaces codes improving on the known general constructions.

## ACKNOWLEDGMENT

The authors wish to thank Michael Kiermaier, University of Bayreuth, for valuable discussions related to this paper and three reviewers for their comments/suggestions on the initial submission.

## REFERENCES

- [1] R. Koetter and F. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.
- [2] F. R. Kschischang, "An introduction to network coding," in *Network Coding: Fundamentals and Applications*, M. Médard and A. Sprintson, Eds. Elsevier Science Publishers, 2012, ch. 1, pp. 1–37.
- [3] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory, Series A*, vol. 25, pp. 226–241, 1978.
- [4] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission*, vol. 21, no. 1, pp. 1–12, 1985.
- [5] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Transactions on Information Theory*, vol. 37, no. 2, pp. 328–336, Mar. 1991, comments by Emst M. Gabidulin and Author's Reply, *ibid.* 38(3):1183, 1992.
- [6] T. Etzion and N. Silberstein, "Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 2909–2919, Jul. 2009.
- [7] —, "Codes and designs related to lifted mrd codes," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1004–1017, Feb. 2013.
- [8] A. Kohnert and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," in *Mathematical Methods in Computer Science. Essays in Memory of Thomas Beth*, ser. Lecture Notes in Computer Science, J. Calmet, W. Geiselmann, and J. Müller-Quade, Eds., no. 5393. Springer-Verlag, 2008, pp. 31–42.
- [9] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1165–1173, Feb. 2011.
- [10] M. Braun and J. Reichelt, " $q$ -analogs of packing designs," *Journal of Combinatorial Designs*, vol. 22, no. 7, pp. 306–321, Jul. 2014, preprint arXiv:1212.4614 [math.CO].
- [11] A. Beutelspacher, "Partial spreads in finite projective spaces and partial designs," *Mathematische Zeitschrift*, vol. 145, pp. 211–230, 1975, corrigendum, *ibid.* 147:303, 1976.
- [12] T. Honold, M. Kiermaier, and S. Kurz, "Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4," Nov. 2013, accepted for publication in the Proceedings of the 11th International Conference on Finite Fields and their Applications (Magdeburg, July 22–26, 2013). Preprint arXiv:1311.0464 [math.CO].
- [13] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wassermann, "Existence of  $q$ -analogs of Steiner systems," Apr. 2013, preprint arXiv:1304.1462 [math.CO].
- [14] P. Dembowski, *Finite Geometries*. Springer-Verlag, 1968, classics in Mathematics Series, 1997.
- [15] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed. Oxford University Press, 1998.
- [16] J. D. Beule and L. Storme, Eds., *Current Research Topics in Galois Geometry*. Nova Science Publishers, 2011.
- [17] S. Thomas, "Designs over finite fields," *Geometriae Dedicata*, vol. 24, pp. 237–242, 1987.
- [18] M. Kiermaier and M. O. Pavčević, "Intersection numbers for subspace designs," may 2014, journal of Combinatorial Designs, accepted for publication.
- [19] D. Silva, F. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.
- [20] A.-L. Trautmann and J. Rosenthal, "New improvements on the Echelon-Ferrers construction," in *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2010)*, A. Edelmayer, Ed., Budapest, Hungary, 5–9 July 2010, pp. 405–408, reprint arXiv:1110.2417 [cs.IT].
- [21] D. M. Mesner, "Sets of disjoint lines in  $PG(3, q)$ ," *Canadian Journal of Mathematics*, vol. 19, pp. 273–280, 1967.